SN 10/588,608

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11238017 A**

(43) Date of publication of application: **31.08.99**

(51) Int. Cl **G06F 12/14**
H04L 9/10

(21) Application number: **10037802**

(22) Date of filing: **19.02.98**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

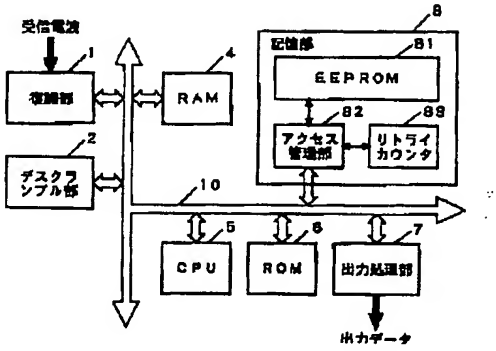
(72) Inventor: **USUKI IZUMI**

(54) **RECEIVER**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a receiver protecting data at the time of illegal access to inner storage information and easily putting a part related to security in an unusable state at the time of abolishment.

SOLUTION: An access monitoring part 82 collates an access code requesting access to EEPROM 81 with a regular access code which the part 82 itself has when it receives the code and judges the matching/non-matching of the access codes. When the access codes are matched with each other by the judgment, access to EEPROM 81 is permitted. When they are not matched, the count value of a retry counter 83 is increased by one without permission and it waits again the input of the access code. When the count value arrives at a previously decided value, the retry counter 83 informs the access monitoring part 82 of the arrival. When the access monitoring part 82 judges the non-matching of the access codes after the notice, it deletes data in EEPROM 81.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－238017

(43)公開日　平成11年(1999)８月31日

(51)Int.Cl.[6]	識別記号	FI	
G06F 12/14	320	G06F 12/14	320D
H04L 9/10		H04L 9/00	621Z

審査請求　未請求　請求項の数11　OL　（全 11 頁）

(21)出願番号　特願平10－37802

(22)出願日　平成10年(1998)２月19日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　薄木　泉
大阪府門真市大字門真1006番地　松下電器産業株式会社内

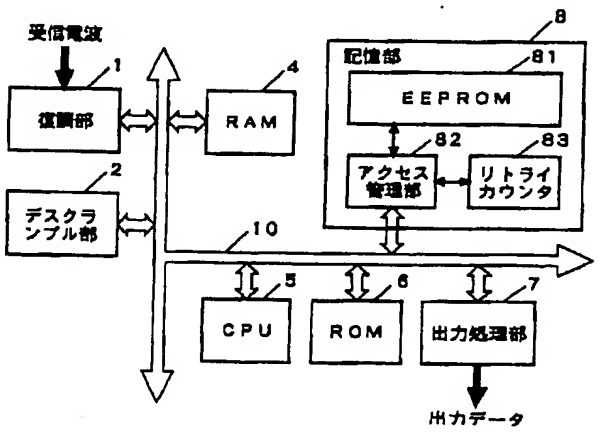
(74)代理人　弁理士　小笠原　史朗

(54)【発明の名称】　受信機

(57)【要約】

【課題】　内部の記憶情報への不正アクセス時にデータを保護し、また廃棄時に容易にセキュリティに関する部分を使用不能な状態にする受信機を提供する。

【解決手段】　アクセス監視部８２は、ＥＥＰＲＯＭ８１へのアクセスを要求するアクセスコードを受付けると、自らが持つ正規のアクセスコードとの照合を行いアクセスコードの一致／不一致を判断する。この判断でアクセスコードが一致した場合は、ＥＥＰＲＯＭ８１へのアクセスを許可するが、不一致の場合には、許可することなくリトライカウンタ８３のカウント値を１つ増加させ、再びアクセスコードの入力を待つ。リトライカウンタ８３は、カウント値が予め定めた値に達するとアクセス監視部８２へその旨を通知する。アクセス監視部８２は、この通知以後、さらにアクセスコードの不一致を判断した場合は、ＥＥＰＲＯＭ８１内のデータの消去を行う。



1

【特許請求の範囲】

【請求項１】　ダウンロードした受信データを電気的書き換え可能な不揮発性半導体メモリ（以下、ＥＥＰＲＯＭという）に格納する受信機であって、

ＣＰＵと、

暗号化された受信データに対し、暗号解読を行うデスクランブル手段と、

前記暗号解読後のデータを格納する前記ＥＥＰＲＯＭと、

前記ＥＥＰＲＯＭに対して要求されるアクセスが正規なアクセスか不正なアクセスかを判断し、当該判断に応じて前記ＥＥＰＲＯＭへのアクセス許可／不許可を制御するアクセス監視手段と、

前記アクセス監視手段に対する不正なアクセスの回数をカウントし、当該カウントの値が予め定めた値に達した場合、前記アクセス監視手段へその旨を通知するリトライカウンタとを少なくとも備え、

前記アクセス監視手段は、前記リトライカウンタから前記通知があった場合、前記ＥＥＰＲＯＭ内のデータを消去することを特徴とする、受信機。

【請求項２】　ダウンロードした受信データを電気的書き換え可能な不揮発性半導体メモリ（以下、ＥＥＰＲＯＭという）に格納する受信機であって、

ＣＰＵと、

暗号化された受信データに対し、暗号解読を行うデスクランブル手段と、

前記暗号解読後のデータを格納する前記ＥＥＰＲＯＭと、

前記ＥＥＰＲＯＭに格納されているデータとは異なるデータが保存された偽データＥＥＰＲＯＭと、

前記ＥＥＰＲＯＭに対して要求されるアクセスが正規なアクセスか不正なアクセスかを判断し、当該判断に応じて前記ＥＥＰＲＯＭまたは前記偽データＥＥＰＲＯＭへのアクセス許可／不許可を制御するアクセス監視手段と、

前記アクセス監視手段に対する不正なアクセスの回数をカウントし、当該カウントの値が予め定めた値に達した場合、前記アクセス監視手段へその旨を通知するリトライカウンタとを少なくとも備え、

前記アクセス監視手段は、前記リトライカウンタから前記通知があった場合、前記偽データＥＥＰＲＯＭに対するアクセス許可を行うことを特徴とする、受信機。

【請求項３】　前記アクセス監視手段は、前記偽データＥＥＰＲＯＭに対するアクセス許可の後、さらに不正なアクセスがあった場合には、前記ＥＥＰＲＯＭ内のデータを消去することを特徴とする、請求項２に記載の受信機。

【請求項４】　ダウンロードした受信データを電気的書き換え可能な不揮発性半導体メモリ（以下、ＥＥＰＲＯＭという）に格納する受信機であって、

2

ＣＰＵと、

暗号化された受信データに対し、暗号解読を行うデスクランブル手段と、

前記暗号解読後のデータを格納する前記ＥＥＰＲＯＭと、

前記ＥＥＰＲＯＭに対して要求されるアクセスが正規なアクセスか不正なアクセスかを判断し、当該判断に応じて前記ＥＥＰＲＯＭへのアクセス許可／不許可を制御するアクセス監視手段と、

前記アクセス監視手段に対する不正なアクセスの回数をカウントし、当該カウントの値が予め定めた値に達した場合、前記アクセス監視手段へその旨を通知するリトライカウンタとを少なくとも備え、

前記アクセス監視手段は、前記リトライカウンタから前記通知があった場合、当該通知以後のアクセスを受付けないことを特徴とする、受信機。

【請求項５】　前記アクセス監視手段は、前記アクセスを受付けない状態に遷移した後であっても、アクセスを行う際の方法とは異なる予め定めた方法によりアクセスの受付けが可能な状態に復帰させることを特徴とする、請求項４に記載の受信機。

【請求項６】　前記アクセス監視手段は、前記異なる予め定めた方法において不正な行為が行われた場合には、前記ＥＥＰＲＯＭ内のデータを消去することを特徴とする、請求項５に記載の受信機。

【請求項７】　受信データを前記ＥＥＰＲＯＭにダウンロードするための動作プログラムを別途記憶する記憶手段をさらに備え、

前記アクセス監視手段は、前記ＥＥＰＲＯＭ内のデータを消去した場合、前記記憶手段に記憶している動作プログラムを前記ＥＥＰＲＯＭに読み出すとともに、同一の受信データを再び受信して前記ＥＥＰＲＯＭにダウンロードすることを特徴とする、請求項１または３若しくは６のいずれかに記載の受信機。

【請求項８】　データに固有の識別情報を付加するＩＤ付加手段をさらに備え、

前記ＥＥＰＲＯＭには、前記固有の識別情報を付加した後のデータを格納することを特徴とする、請求項１～７のいずれかに記載の受信機。

【請求項９】　前記デスクランブル手段は、電気的に書き換え可能な素子を用いて回路が構成されており、

前記アクセス監視手段は、前記リトライカウンタから前記通知があった場合、前記ＥＥＰＲＯＭ内のデータを消去するとともに、前記デスクランブル手段の回路を消去することを特徴とする、請求項１～８のいずれかに記載の受信機。

【請求項１０】　前記デスクランブル手段は、電気的に書き換え可能な素子を用いて回路が構成されており、

前記ＣＰＵは、外部からの指示に従って、前記ＥＥＰＲＯＭ内のデータの消去、および前記デスクランブル手段

の回路の消去を行うことを特徴とする、請求項１～９のいずれかに記載の受信機。

【請求項１１】　送信されるデータを受信し、当該受信したデータを内部に格納または外部へ出力する受信機であって、

送信されるデータを受信する受信手段と、

前記受信手段から出力されるデータに固有の識別情報を付加するＩＤ付加手段と、

前記固有の識別情報が付加されたデータを内部に格納または外部へ出力する処理手段とを少なくとも備える、受信機。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、受信機に関し、より特定的には、衛星通信システムやインターネット等において伝送されるデジタル画像，ソフトウエア等をダウンロードしたデータに対し、第三者の不正盗用を防止する受信機に関する。

【０００２】

【従来の技術】図１２に、従来の受信機の構成の一例として、デジタル衛星通信システム等で受信機として使用されるインテリジェント・レシーバー・デコーダ（Intelligent Receiver and Decoder）のブロック図を示す。図１２において、従来の受信機は、復調部１０１と、デスクランブル部１０２と、ランダム・アクセス・メモリ（ＲＡＭ）１０４と、中央演算処理装置（ＣＰＵ）１０５と、リード・オンリー・メモリ（ＲＯＭ）１０６と、出力処理部１０７と、ＥＥＰＲＯＭ（Electrically Erasable and Programmable ＲＯＭ）１８１とを備える。これらの各構成は、バス１１０により相互に接続されている。

【０００３】衛星から受信した電波は、復調部１０１でデジタル符号データに変換される。変換されたデジタル符号データは、デスクランブル部１０２において予め定めた規則の下暗号を解読される。暗号解読後のデータは、通常、ＲＡＭ１０４に一旦格納され（ただし、受信データが連続している場合には、ＲＡＭ１０４に格納することなく直ちに出力処理部７を介して出力することもある）、その後、出力処理部１０７を介してテレビ受像器やパーソナル・コンピュータ等の外部端末（以下、外部ＰＣと称する）へ出力される（図示せず）。ここで、受信データが受信機のシステムソフトダウンロード用のデータであった場合、ＣＰＵ１０５は、ＲＡＭ１０４に格納された暗号解読後のデータをさらにＥＥＰＲＯＭ１８１に記憶する。

【０００４】なお、上記受信データが、例えば、ＭＰＥＧ２（Moving Picture Experts Group 2）方式のデータである場合には、暗号解読後に内蔵するＭＰＥＧ２デコード部（図示せず）によってデータがデコードされる。

【０００５】このように、通常、データはメモリ（ＲＡＭ１０４，ＥＥＰＲＯＭ１８１）に格納され、その後外部ＰＣに出力する等、ユーザが自由に使用することができる。特に、衛星通信における上記従来の受信機では、システムソフトは、衛星回線からのダウンロードによっていつでも更新が可能なようにＥＥＰＲＯＭ１８１に格納されている。

【０００６】

【発明が解決しようとする課題】上述したように、従来の受信機は、受信したデータをメモリに格納している。しかし、従来の受信機は、これらの格納データに対し何らセキュリティ対策を施していないため、第三者の不正アクセスにより格納データが容易にコピーされてしまう。特に、コピーされた格納データが著作権のあるデータの場合には、著作権侵害等の問題が発生してしまう。

【０００７】また、受信機内のＥＥＰＲＯＭ１８１に格納されているデータは、受信機を分解して直接ＥＥＰＲＯＭ１８１を読み出すことによっても第三者が自由に得ることができ、これによっても著作権侵害等の問題が発生してしまう。このため、通常、受信機の廃棄の際には、廃棄物を解析されても問題がないように受信機のセキュリティに関連するデバイスを完全に使用不能状態にしてから廃棄する。しかし、このようにデバイスを完全に使用不能状態にするには、手間やコストがかかる等の問題がある。

【０００８】それ故、本発明の目的は、受信機内に記憶している情報への不正アクセス時にデータを保護し、また、廃棄時に容易にセキュリティに関する部分を使用不能な状態にすることが可能な受信機を提供することである。

【０００９】

【課題を解決するための手段および発明の効果】第１の発明は、ダウンロードした受信データを電気的書き換え可能な不揮発性半導体メモリ（以下、ＥＥＰＲＯＭという）に格納する受信機であって、ＣＰＵと、暗号化された受信データに対し、暗号解読を行うデスクランブル手段と、暗号解読後のデータを格納するＥＥＰＲＯＭと、ＥＥＰＲＯＭに対して要求されるアクセスが正規なアクセスか不正なアクセスかを判断し、当該判断に応じてＥＥＰＲＯＭへのアクセス許可／不許可を制御するアクセス監視手段と、アクセス監視手段に対する不正なアクセスの回数をカウントし、当該カウントの値が予め定めた値に達した場合、アクセス監視手段へその旨を通知するリトライカウンタとを少なくとも備え、アクセス監視手段は、リトライカウンタから通知があった場合、ＥＥＰＲＯＭ内のデータを消去することを特徴とする。

【００１０】上記のように、第１の発明によれば、第三者の不正アクセスがあった場合、予め定めた回数に達すると自動的にＥＥＰＲＯＭ内のデータを消去する。これにより、第三者への情報の漏洩防止を図ることができる。

5

【００１１】第２の発明は、ダウンロードした受信データを電気的書き換え可能な不揮発性半導体メモリ（以下、ＥＥＰＲＯＭという）に格納する受信機であって、ＣＰＵと、暗号化された受信データに対し、暗号解読を行うデスクランブル手段と、暗号解読後のデータを格納するＥＥＰＲＯＭと、ＥＥＰＲＯＭに格納されているデータとは異なるデータが保存された偽データＥＥＰＲＯＭと、ＥＥＰＲＯＭに対して要求されるアクセスが正規なアクセスか不正なアクセスかを判断し、当該判断に応じてＥＥＰＲＯＭまたは偽データＥＥＰＲＯＭへのアクセス許可／不許可を制御するアクセス監視手段と、アクセス監視手段に対する不正なアクセスの回数をカウントし、当該カウントの値が予め定めた値に達した場合、アクセス監視手段へその旨を通知するリトライカウンタとを少なくとも備え、アクセス監視手段は、リトライカウンタから通知があった場合、偽データＥＥＰＲＯＭに対するアクセス許可を行うことを特徴とする。

【００１２】上記のように、第２の発明によれば、第三者の不正アクセスがあった場合、予め定めた回数に達すると自動的に偽データを出力する。これにより、ＥＥＰＲＯＭ内のデータを消去することなく、第三者への情報の漏洩防止を図ることができる。

【００１３】第３の発明は、第２の発明において、アクセス監視手段は、偽データＥＥＰＲＯＭに対するアクセス許可の後、さらに不正なアクセスがあった場合には、ＥＥＰＲＯＭ内のデータを消去することを特徴とする。

【００１４】上記のように、第３の発明によれば、第２の発明において、出力したデータが偽データであると判断されても、その後に不正アクセスがあった場合には、自動的にＥＥＰＲＯＭ内のデータを消去する。従って、第１の発明と同様に、確実に第三者への情報の漏洩防止を図ることができる。

【００１５】第４の発明は、ダウンロードした受信データを電気的書き換え可能な不揮発性半導体メモリ（以下、ＥＥＰＲＯＭという）に格納する受信機であって、ＣＰＵと、暗号化された受信データに対し、暗号解読を行うデスクランブル手段と、暗号解読後のデータを格納するＥＥＰＲＯＭと、ＥＥＰＲＯＭに対して要求されるアクセスが正規なアクセスか不正なアクセスかを判断し、当該判断に応じてＥＥＰＲＯＭへのアクセス許可／不許可を制御するアクセス監視手段と、アクセス監視手段に対する不正なアクセスの回数をカウントし、当該カウントの値が予め定めた値に達した場合、アクセス監視手段へその旨を通知するリトライカウンタとを少なくとも備え、アクセス監視手段は、リトライカウンタから通知があった場合、当該通知以後のアクセスを受付けないことを特徴とする。

【００１６】上記のように、第４の発明によれば、第三者の不正アクセスがあった場合、予め定めた回数に達するとアクセスを受付けない状態にする。これにより、第三者への情報の漏洩防止を図ることができる。

6

【００１７】第５の発明は、第４の発明において、アクセス監視手段は、アクセスを受付けない状態に遷移した後であっても、アクセスを行う際の方法とは異なる予め定めた方法によりアクセスの受付けが可能な状態に復帰させることを特徴とする。

【００１８】上記のように、第５の発明によれば、第４の発明において、アクセスする方法とは異なる方法を用いて状態を復帰できるようにする。これにより、正規のユーザは、容易に元の状態に復帰させることができる。

【００１９】第６の発明は、第５の発明において、アクセス監視手段は、異なる予め定めた方法において不正な行為が行われた場合には、ＥＥＰＲＯＭ内のデータを消去することを特徴とする。

【００２０】上記のように、第６の発明によれば、第５の発明において、異なる方法の存在を知られても不正な行為を行った場合には、自動的にＥＥＰＲＯＭ内のデータを消去する。従って、第１の発明と同様に、確実に第三者への情報の漏洩防止を図ることができる。

【００２１】第７の発明は、第１，第３および第６の発明において、受信データをＥＥＰＲＯＭにダウンロードするための動作プログラムを別途記憶する記憶手段をさらに備え、アクセス監視手段は、ＥＥＰＲＯＭ内のデータを消去した場合、記憶手段に記憶している動作プログラムをＥＥＰＲＯＭに読み出すとともに、同一の受信データを再び受信してＥＥＰＲＯＭにダウンロードすることを特徴とする。

【００２２】上記のように、第７の発明によれば、第１，第３および第６の発明において、ダウンロードに必要な動作プログラムを記録した記憶手段をさらに備えている。これにより、ＥＥＰＲＯＭ内のデータを消去しても、その後、記憶手段から動作プログラムを読み込むことにより消去したデータを復元することができる。

【００２３】第８の発明は、第１～第７の発明において、データに固有の識別情報を付加するＩＤ付加手段をさらに備え、ＥＥＰＲＯＭには、固有の識別情報を付加した後のデータを格納することを特徴とする。

【００２４】上記のように、第８の発明によれば、第１～第７の発明において、データに固有の識別情報を付加するＩＤ付加手段をさらに備える。これにより、万一データが不正に盗用されたても、付加された固有の識別情報から盗用データであると判断することができる。従って、第三者の不正行為の摘発が容易になり、ひいては事前に不正行為を抑制するという効果がある。

【００２５】第９の発明は、第１～第８の発明において、デスクランブル手段は、電気的に書き換え可能な素子を用いて回路が構成されており、アクセス監視手段は、リトライカウンタから通知があった場合、ＥＥＰＲＯＭ内のデータを消去するとともに、デスクランブル手段の回路を消去することを特徴とする。

【００２６】上記のように、第９の発明によれば、第１～第８の発明において、デスクランブル手段の回路を電気的に書き換え可能な素子を用いて構成する。そして、第三者の不正アクセスがあった場合、予め定めた回数に達すると自動的にＥＥＰＲＯＭ内のデータを消去し、かつ、デスクランブル手段の回路を電気的に消去する。これにより、第三者への情報の漏洩防止を図ることができるとともに、セキュリティに関連する情報の漏洩防止を図ることができる。

【００２７】第１０の発明は、第１～第９の発明において、デスクランブル手段は、電気的に書き換え可能な素子を用いて回路が構成されており、ＣＰＵは、外部からの指示に従って、ＥＥＰＲＯＭ内のデータの消去、およびデスクランブル手段の回路の消去を行うことを特徴とする。

【００２８】上記のように、第１０の発明によれば、第１～第９の発明において、デスクランブル手段の回路を電気的に書き換え可能な素子を用いて構成する。そして、外部からの指示によりＥＥＰＲＯＭ内のデータの消去、およびデスクランブル手段の回路の電気的消去を行えるようにする。これにより、廃棄時においても、確実にセキュリティに関連する情報の漏洩防止を図ることができる。

【００２９】第１１の発明は、送信されるデータを受信し、当該受信したデータを内部に格納または外部へ出力する受信機であって、送信されるデータを受信する受信手段と、受信手段から出力されるデータに固有の識別情報を付加するＩＤ付加手段と、固有の識別情報が付加されたデータを内部に格納または外部へ出力する処理手段とを少なくとも備える。

【００３０】上記のように、第１１の発明によれば、データに固有の識別情報を付加した後、内部に格納または外部へ出力する。これにより、データがどの受信機から取得されたものかを判断することができる。従って、第三者の不正行為を事前に抑制するとともに、第三者の不正行為があった場合は摘発が容易になる。

【００３１】

【発明の実施の形態】以下、本発明の実施形態について、デジタル衛星通信システム等で受信機として使用されるインテリジェント・レシーバー・デコーダを一例に挙げて説明する。

【００３２】（第１の実施形態）図１は、本発明の第１の実施形態に係る受信機の構成を示すブロック図である。図１において、本第１の実施形態に係る受信機は、復調部１と、デスクランブル部２と、ＲＡＭ４と、ＣＰＵ５と、ＲＯＭ６と、出力処理部７と、記憶部８とを備える。これらの各構成は、バス１０によって相互に接続されている。また、記憶部８は、ＥＥＰＲＯＭ８１と、アクセス監視部８２と、リトライカウンタ８３とを備える。

【００３３】復調部１は、受信データをデジタル符号データに変換する。デスクランブル部２は、復調部１でデジタル符号化したデータの暗号を解読する。ＲＡＭ４は、データを格納する。ＣＰＵ５は、受信機全体の制御を行う。また、ＣＰＵ５は、アクセスに必要な予め定めたアクセスコードを記憶している。ＲＯＭ６は、受信機が行う制御プログラムを格納している。出力処理部７は、デスクランブル部２の出力をテレビ受像器等（図示せず）へ出力する。ＥＥＰＲＯＭ８１は、上記受信データが受信機のシステムソフトダウンロード用のデータであった場合、当該データを記憶する。アクセス監視部８２は、アクセスに必要な予め定めたアクセスコードを記憶している。なお、上記ＣＰＵ５が記憶するアクセスコードとアクセス監視部８２が記憶するアクセスコードとは同じものである。リトライカウンタ８３は、アクセス監視部８２が行うアクセスコードの照合回数をカウントする。

【００３４】衛星から電波として受信されたデータは、復調部１においてデジタル符号データに変換される。変換されたデジタル符号データは、デスクランブル部２において予め定めた規則の下、暗号が解読される。暗号解読後のデータは、通常、ＲＡＭ４に一旦格納され（ただし、受信データが連続している場合には、ＲＡＭ４に格納することなく直ちに出力処理部７を介して出力することもある）、その後、出力処理部７を介して外部ＰＣ（図示せず）へ出力される。なお、上記受信データが、例えば、ＭＰＥＧ２方式のデータである場合には、内蔵するＭＰＥＧ２デコード部（図示せず）によって暗号解読後のデータがデコードされる。

【００３５】ここで、受信データが受信機のシステムソフトダウンロード用のデータであった場合、ＣＰＵ５は、ＲＡＭ４に格納された暗号解読後のデータをさらにＥＥＰＲＯＭ８に記憶すべく、アクセス監視部８２へアクセスを行う。

【００３６】このＣＰＵ５とアクセス監視部８２との間のアクセスは、まず、ＣＰＵ５が自らが記憶するアクセスコードを、アクセス監視部８２へ通知する。そして、アクセス監視部８２は、ＣＰＵ５から通知されたアクセスコードと、アクセス監視部８２自らが記憶しているアクセスコードとを照合し、一致した場合にのみＥＥＰＲＯＭ８１へのアクセスを許可する。従って、正常なアクセスの場合には、ＣＰＵ５およびＥＥＰＲＯＭ８１の双方のアクセスコードが同一であるため、問題なくアクセスが可能となる。

【００３７】一方、不正行為を行う第三者は、自らの機器（以下、不正機器と称する）を使用してＥＥＰＲＯＭ８１の内容を読み取ろうとする。この場合、第三者が行うアクセスは、不正機器内のＣＰＵを使用して行われることになる。従って、このような不正行為が行われても、不正機器内のＣＰＵがアクセスコードを通知する必

9

要があることを知らないため、また、通知する必要があること知っていても不正機器のＣＰＵが固有に記憶する誤ったアクセスコードであるため、アクセス監視部８２がこのアクセスを拒絶する（アクセスコードを照合しても、一致しないからである）。これに対して、第三者は、何回か異なる任意のアクセスコードを試みると考えられる。しかし、リトライカウンタ８３は、アクセス監視部８２がアクセスを拒絶した回数をカウントしており、予め定めた回数が行われたときにはアクセス監視部８２へその旨を通知する。この通知を受けたアクセス監視部８２は、最終的な対応として、ＥＥＰＲＯＭ８１内の格納データを消去する。

【００３８】このように、アクセスを試みることができる回数を予め制限することで、不正行為を行う第三者のアクセスコードが正規のアクセスコードと合致する確率をきわめて低くできる（もちろん、アクセスコードのビット数にも関係する）。

【００３９】以下、上記構成による第１の実施形態に係る受信機の不正アクセスに対する動作を、図２を参照しつつ説明する。図２は、本発明の第１の実施形態に係る受信機における状態遷移を示す図である。図２においては、リトライカウンタ８３がアクセス監視部８２へ通知を行うカウント数を「３」としている。

【００４０】まず、初期状態として、アクセス監視部８２は、アクセスコードを受け付ける第１のアクセスコード待ち状態にある（状態Ｓ１）。また、リトライカウンタ８３は、初期値「０」であるとする。ある者がアクセスを試みる（トライ）、すなわち、アクセスコードが通知されてくると、アクセス監視部８２は、通知されたアクセスコードと自ら記憶しているアクセスコードとを照合する。ここで、通知されたアクセスコードが正規のものである場合、アクセス監視部８２は、アクセスを許可する。

【００４１】一方、通知されたアクセスコードが不正なものである場合、アクセス監視部８２は、アクセスコード不一致と判断し、リトライカウンタ８３を１つ増加させ「１」とする。このときは、まだ状態Ｓ１にあり、再びアクセスコードを受け付ける状態となる。再び不正アクセスコードが入力されると、アクセス監視部８２は、またアクセスコード不一致と判断し、さらにリトライカウンタ８３を１つ増加させ「２」とする。同様に、状態Ｓ１において、再び不正アクセスコードが入力されると、アクセス監視部８２は、アクセスコード不一致と判断し、さらにリトライカウンタ８３を１つ増加させ「３」とする。ここで、リトライカウンタ８３のカウント値が「３」に達したため、リトライカウンタ８３は、アクセス監視部８２へその旨を通知する。アクセス監視部８２は、この通知を受けて第２のアクセスコード待ち状態へ遷移する（状態Ｓ２）。

【００４２】状態Ｓ２において、再び不正アクセスコードが入力されると、アクセス監視部８２は、アクセスコード不一致と判断するとともに、ＥＥＰＲＯＭ８１内の格納データを消去する（状態Ｓ３）。一方、状態Ｓ２において、正規のアクセスコードが入力された場合は、アクセス監視部８２は、アクセスを許可するとともに、状態Ｓ１へ遷移させ、さらにリトライカウンタ８３のカウント値をリセットする。

【００４３】以上のように、本発明の第１の実施形態に係る受信機は、不正アクセスの回数をカウントし、予め定めた回数が行われた場合には、ＥＥＰＲＯＭ８１内の格納データを消去する。これにより、アクセスコードを知らない第三者の不正アクセス行為があった場合、データ漏洩防止を図ることができる。

【００４４】（第２の実施形態）図３は、本発明の第２の実施形態に係る受信機の構成を示すブロック図である。図３において、本第２の実施形態に係る受信機は、復調部１と、デスクランブル部２と、ＲＡＭ４と、ＣＰＵ５と、ＲＯＭ６と、出力処理部７と、記憶部８ａとを備える。これらの各構成は、バス１０によって相互に接続されている。また、記憶部８ａは、ＥＥＰＲＯＭ８１と、アクセス監視部８２と、リトライカウンタ８３と、偽データＥＥＰＲＯＭ８４とを備える。

【００４５】図３に示すように、本第２の実施形態に係る受信機の記憶部８ａは、上記第１の実施形態に係る受信機の記憶部８に偽データＥＥＰＲＯＭ８４をさらに加えた構成である。偽データＥＥＰＲＯＭ８４は、ＥＥＰＲＯＭ８１に格納しているデータとは異なる偽のデータを格納している。なお、本第２の実施形態に係る受信機のその他の構成は、上記第１の実施形態に係る受信機の構成と同様であり、当該構成については同一の参照番号を付してその説明を省略する。

【００４６】第２の実施形態に係る受信機は、アクセス監視部８２がリトライカウンタ８３から通知を受けた場合、最終的な対応としてＥＥＰＲＯＭ８１内の格納データを消去する前に、偽データを出力する。

【００４７】以下、上記構成による第２の実施形態に係る受信機の不正アクセスに対する動作を、図４を参照しつつ説明する。図４は、本発明の第２の実施形態に係る受信機における状態遷移を示す図である。図４においては、リトライカウンタ８３がアクセス監視部８２へ通知を行うカウント数を「３」としている。なお、状態Ｓ１および状態Ｓ３は、上記第１の実施形態に係る受信機の場合と同様であるため、その説明は省略する。

【００４８】リトライカウンタ８３は、カウント値が「３」に達するとアクセス監視部８２へその旨を通知する。アクセス監視部８２は、この通知を受けて、外部からはあたかも正規のアクセスコードに合致したかのように偽データＥＥＰＲＯＭ８４に格納している偽データを出力する（状態Ｓ４）。

【００４９】このとき、第三者が偽データだと気づい

て、再び不正アクセスコードが入力されると、アクセス監視部８２は、アクセスコード不一致と判断するとともに、ＥＥＰＲＯＭ８１内の格納データを消去する（状態Ｓ３）。一方、状態Ｓ４において、正規のアクセスコードが入力された場合は、アクセス監視部８２は、アクセスを許可するとともに、状態Ｓ４から状態Ｓ１へ遷移させ、さらにリトライカウンタ８３のカウント値をリセットする。

【００５０】なお、状態Ｓ４から状態Ｓ３への遷移は、１回の不正アクセスですぐに行うようにするほか、状態Ｓ１から状態Ｓ４への遷移と同様に、リトライカウンタ８３を使用して予め定めた回数の不正アクセスがあった場合に行うようにしてもよい（図１１を参照）。

【００５１】以上のように、本発明の第２の実施形態に係る受信機は、不正アクセスの回数をカウントし、予め定めた回数が行われた場合には、ＥＥＰＲＯＭ８１内の格納データを消去する前に、まず偽のデータを出力する。これにより、アクセスコードを知らない第三者の不正アクセス行為があった場合、格納データの消去を極力避けつつもデータ漏洩防止を図ることができる。

【００５２】（第３の実施形態）図５は、本発明の第３の実施形態に係る受信機の構成を示すブロック図である。図５において、本第３の実施形態に係る受信機は、復調部１と、デスクランブル部２と、ＲＡＭ４と、ＣＰＵ５と、ＲＯＭ６と、出力処理部７と、記憶部８とを備える。これらの各構成は、バス１０によって相互に接続されている。また、記憶部８は、ＥＥＰＲＯＭ８１と、アクセス監視部８２と、リトライカウンタ８３とを備える。

【００５３】図５に示すように、本第３の実施形態に係る受信機は、構成的には上記第１の実施形態に係る受信機と同様の構成である。本第３の実施形態に係る受信機が上記第１の実施形態に係る受信機と異なる点は、図２における状態Ｓ２で行う処理である。なお、本第３の実施形態に係る受信機のその他の構成は、上記第１の実施形態に係る受信機の構成と同様であり、当該構成については同一の参照番号を付してその説明を省略する。

【００５４】以下、上記構成による第３の実施形態に係る受信機の不正アクセスに対する動作を、図６を参照しつつ説明する。図６は、本発明の第３の実施形態に係る受信機における状態遷移を示す図である。図６においては、リトライカウンタ８３がアクセス監視部８２へ通知を行うカウント数を「３」としている。なお、状態Ｓ１および状態Ｓ３は、上記第１の実施形態に係る受信機の場合と同様であるため、その説明は省略する。

【００５５】リトライカウンタ８３は、カウント値が「３」に達するとアクセス監視部８２へその旨を通知する。アクセス監視部８２は、この通知を受けて、アクセスコードの受付けを完全に拒絶する（状態Ｓ５）。ここで、この状態Ｓ５にある場合、復帰コード（アクセスコードとは別の信号線を規定の状態にするコード）の入力により復帰できるようにする。すなわち、状態Ｓ５において、正規のアクセスコードが入力された場合には、状態Ｓ１へ遷移するようにする。一方、第三者が復帰コードの存在を知っていても、正規の復帰コードまでを知り得ることは希であり、不正な復帰コードで再び試みた場合には、上記と同様にＥＥＰＲＯＭ８１内の格納データを消去する（状態Ｓ３）。このような処理を行うことで、状態Ｓ５のまま第三者が不正アクセスを断念した場合には、正規のユーザが復帰コードを入力することで、容易に状態Ｓ１へ遷移させることができる。

【００５６】なお、状態Ｓ５から状態Ｓ３への遷移は、１回の不正な復帰コードの入力によりすぐに行うようにする他、状態Ｓ１から状態Ｓ５への遷移と同様に、リトライカウンタ８３を使用して予め定めた回数の不正な復帰コードの入力があった場合に行うようにしてもよい。

【００５７】以上のように、本発明の第３の実施形態に係る受信機は、不正アクセスの回数をカウントし、予め定めた回数が行われた場合には、アクセスを完全に拒絶し、極秘の復帰コードの受付け状態にする。これにより、アクセスコードを知らない第三者の不正アクセス行為があった場合、格納データの消去を極力避けつつもデータ漏洩防止を図ることができる。

【００５８】（第４の実施形態）図７は、本発明の第４の実施形態に係る受信機の構成を示すブロック図である。図７において、本第４の実施形態に係る受信機は、復調部１と、デスクランブル部２と、ＲＡＭ４と、ＣＰＵ５と、ＲＯＭ６と、出力処理部７と、記憶部８とを備える。これらの各構成は、バス１０によって相互に接続されている。また、記憶部８は、ＥＥＰＲＯＭ８１と、アクセス監視部８２と、リトライカウンタ８３とを備える。

【００５９】図７に示すように、本第４の実施形態に係る受信機は、構成的には上記第１の実施形態に係る受信機と同様の構成である。本第４の実施形態に係る受信機が上記第１の実施形態に係る受信機と異なるのは、ＲＯＭ６内にダウンロードに関するソフトウエアのすべて（以下、ダウンロードモジュールという）を格納する部分ＤＭ６１を有している点である。このＤＭ６１へのダウンロードモジュールの格納は、例えば、受信機の出荷段階で行えばよい。なお、本第５の実施形態に係る受信機のその他の構成は、上記第１の実施形態に係る受信機の構成と同様であり、当該構成については同一の参照番号を付してその説明を省略する。

【００６０】以下、上記構成による第５の実施形態に係る受信機の不正アクセスに対する動作を説明する。リトライカウンタ８３は、カウント値が「３」に達するとアクセス監視部８２へその旨を通知する。アクセス監視部８２は、この通知を受けて、第２のアクセスコード待ち状態へ遷移する（図２における状態Ｓ２を参照）。状態

13

Ｓ２において、再び不正アクセスコードが入力されると、アクセス監視部８２は、アクセスコード不一致と判断するとともに、ＥＥＰＲＯＭ８１内の格納データを消去する。その後、アクセス監視部８２は、ダウンロードモジュールをＲＯＭ６内のＤＭ６１から読み出して再びＥＥＰＲＯＭ８１内に格納する処理を自動的に行う。

【００６１】以上のように、本発明の第４の実施形態に係る受信機は、不正アクセスの回数をカウントし、予め定めた回数が行われた場合には、ＥＥＰＲＯＭ８１内の格納データを消去する。そして、その後、消去した格納データのうちダウンロードモジュールのみを自動的に復元する。これにより、アクセスコードを知らない第三者の不正アクセス行為によりＥＥＰＲＯＭ８１内の格納データが消去された場合でも、衛星から送られてくる同一データを再び受信してＥＥＰＲＯＭ８１に再格納することで、容易に消去データの復元を行うことができる。

【００６２】なお、本第４の実施形態において示したＲＯＭ６内のＤＭ６１にダウンロードモジュールを格納する構成は、上記第１の実施形態に係る受信機のみならず上記第２および第３の実施形態に係る受信機においても同様に用いることが可能である。

【００６３】（第５の実施形態）図８は、本発明の第５の実施形態に係る受信機の構成を示すブロック図である。図８において、本第５の実施形態に係る受信機は、復調部１と、デスクランブル部２と、ＲＡＭ４と、ＣＰＵ５と、ＲＯＭ６と、出力処理部７と、記憶部８と、ＩＤ（identification）付加部９とを備える。これらの各構成は、バス１０によって相互に接続されている。また、記憶部８は、ＥＥＰＲＯＭ８１と、アクセス監視部８２と、リトライカウンタ８３とを備える。

【００６４】図８に示すように、本第５の実施形態に係る受信機は、上記第１の実施形態に係る受信機に、ＩＤ付加部３を加えたものである。ＩＤ付加部３は、受信機固有のＩＤ情報を電子すかしの手法で受信データ内に埋め込む処理を行う。なお、本第５の実施形態に係る受信機のその他の構成は、上記第１の実施形態に係る受信機の構成と同様であり、当該構成については同一の参照番号を付してその説明を省略する。

【００６５】ＩＤ付加部３においてＩＤ情報を埋め込むデータは、ＲＡＭ４に格納される前のデータであってもよいし、外部ＰＣ等へ出力する際にＲＡＭ４から読み出されるデータであってもよい。

【００６６】以上のように、本発明の第５の実施形態に係る受信機は、データ保護の処理を行う前に受信データに受信機固有のＩＤ情報を埋め込む。これにより、万一アクセスコードが一致して第三者に不正にデータが盗用されても、埋め込まれたＩＤ情報からデータが不正盗用されたものであるという判断ができる。従って、第三者の不正行為の摘発が容易になり、ひいては事前に不正行為を抑制するという効果がある。

14

【００６７】なお、本第５の実施形態において示した受信データに受信機固有のＩＤ情報を埋め込む手法は、上記第１の実施形態に係る受信機のみならず上記第２～第４の実施形態に係る受信機においても同様に用いることが可能である。また、本第５の実施形態において示した受信データに受信機固有のＩＤ情報を埋め込む手法は、必ずしも上記第１～第４の実施形態とともに使用しなければならないものではなく、事前に不正行為を抑制するという意味において単独で用いることも可能である。

【００６８】（第６の実施形態）図９は、本発明の第６の実施形態に係る受信機の構成を示すブロック図である。図９において、本第６の実施形態に係る受信機は、復調部１と、ＦＰＧＡ(Field Programmable gate array) デスクランブル部２ａと、ＲＡＭ４と、ＣＰＵ５と、ＲＯＭ６と、出力処理部７と、記憶部８とを備える。これらの各構成は、バス１０によって相互に接続されている。また、記憶部８は、ＥＥＰＲＯＭ８１と、アクセス監視部８２と、リトライカウンタ８３とを備える。

【００６９】図９に示すように、本第６の実施形態に係る受信機は、上記第１の実施形態に係る受信機のデスクランブル部２を、ＦＰＧＡデスクランブル部２ａに代えたものである。また、ＦＰＧＡデスクランブル部２ａの内部回路を書き換えるための専用の信号線２６が、アクセス監視部８２からＦＰＧＡデスクランブル部２ａへ接続されている。なお、本第６の実施形態に係る受信機のその他の構成は、上記第１の実施形態に係る受信機の構成と同様であり、当該構成については同一の参照番号を付してその説明を省略する。

【００７０】ＦＰＧＡデスクランブル部２ａとは、ＦＰＧＡによって回路構成されたデスクランブル部である。そして、ＦＰＧＡとは、外部からの電気的処理により回路プログラムが可能なゲートアレーをいう。従って、ＦＰＧＡ回路は、電気的に消去することも可能なのである。

【００７１】以下、上記構成による第６の実施形態に係る受信機の不正アクセスに対する動作を説明する。リトライカウンタ８３は、カウント値が「3」に達するとアクセス監視部８２へその旨を通知する。アクセス監視部８２は、この通知を受けて、第２のアクセスコード待ち状態へ遷移する（図２における状態Ｓ２を参照）。状態Ｓ２において、再び不正アクセスコードが入力されると、アクセス監視部８２は、アクセスコード不一致と判断するとともに、ＥＥＰＲＯＭ８１内の格納データを消去し、かつ、信号線２６を使用してＦＰＧＡデスクランブル部２ａのＦＰＧＡ回路データを消去する。

【００７２】以上のように、本発明の第６の実施形態に係る受信機は、デスクランブル部をＦＰＧＡ回路で構成する。さらに、不正アクセスの回数をカウントし、予め定めた回数が行われた場合には、ＥＥＰＲＯＭ８１内の

15

格納データとともにＦＰＧＡデスクランブル部２ａのＦＰＧＡ回路データをも消去する。これにより、アクセスコードを知らない第三者の不正アクセス行為があった場合、ＥＥＰＲＯＭ８１内の格納データを消去することによりデータ漏洩防止を図るとともに、暗号解読を行うＦＰＧＡデスクランブラ部２ａの回路をも消去するため、セキュリティに関連する情報の漏洩防止も図ることができる。

【００７３】なお、本第６の実施形態において示したデスクランブル部をＦＰＧＡ回路によって構成することは、上記第１の実施形態に係る受信機のみならず上記第２～第５の実施形態に係る受信機においても同様に用いることが可能である。

【００７４】（第７の実施形態）図１０は、本発明の第７の実施形態に係る受信機の構成を示すブロック図である。図１０において、本第７の実施形態に係る受信機は、復調部１と、ＦＰＧＡデスクランブル部２ａと、ＲＡＭ４と、ＣＰＵ５と、ＲＯＭ６と、出力処理部７と、記憶部８とを備える。これらの各構成は、バス１０によって相互に接続されている。また、記憶部８は、ＥＥＰＲＯＭ８１と、アクセス監視部８２と、リトライカウンタ８３とを備える。

【００７５】図１０に示すように、本第７の実施形態に係る受信機は、上記第１の実施形態に係る受信機のデスクランブル部２を、ＦＰＧＡデスクランブル部２ａに代えたものである。また、ＦＰＧＡデスクランブル部２ａの内部回路を書き換えるための専用の信号線２７が、ＣＰＵ５からＦＰＧＡデスクランブル部２ａへ接続されている。なお、本第７の実施形態に係る受信機のその他の構成は、上記第１の実施形態に係る受信機の構成と同様であり、当該構成については同一の参照番号を付してその説明を省略する。

【００７６】上記構成による第７の実施形態に係る受信機は、不正アクセスに対するデータ保護動作は上記第１～第６の実施形態に係る受信機と同様であるが、廃棄時の処理が異なる。すなわち、受信機の廃棄時に、ＣＰＵ５から再度ＥＥＰＲＯＭ８１内の格納データを消去するとともに、信号線２７を使用してＦＰＧＡデスクランブル部２ａのＦＰＧＡ回路データを消去するのである。

【００７７】以上のように、本発明の第７の実施形態に係る受信機は、デスクランブル部をＦＰＧＡ回路で構成する。そして、受信機の廃棄時には、ＣＰＵ５からＥＥＰＲＯＭ８１内の格納データおよびＦＰＧＡデスクランブル部２ａのＦＰＧＡ回路データの消去を行う。これにより、セキュリティに関連するデータおよび機能をすべて使用不能とした後に受信機を廃棄することができ、セキュリティに関連する情報の漏洩防止をより確実に図ることができる。

【００７８】なお、本第７の実施形態において示したＥ

16

ＥＰＲＯＭ８１内の格納データおよびＦＰＧＡデスクランブル部２ａのＦＰＧＡ回路データを受信機の廃棄時に消去する処理は、上記第１の実施形態に係る受信機のみならず上記第２～第６の実施形態に係る受信機においても同様に用いることが可能である。

【００７９】また、本発明に係る受信機は、上記第１～第７の実施形態で示したように無線の通信システムにのみ用いられるものではなく、インターネット等の有線による通信システムにも同様に用いることができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係る受信機の構成を示すブロック図である。

【図２】本発明の第１の実施形態に係る受信機における状態遷移を示す図である。

【図３】本発明の第２の実施形態に係る受信機の構成を示すブロック図である。

【図４】本発明の第２の実施形態に係る受信機における状態遷移を示す図である。

【図５】本発明の第３の実施形態に係る受信機の構成を示すブロック図である。

【図６】本発明の第３の実施形態に係る受信機における状態遷移を示す図である。

【図７】本発明の第４の実施形態に係る受信機の構成を示すブロック図である。

【図８】本発明の第５の実施形態に係る受信機の構成を示すブロック図である。

【図９】本発明の第６の実施形態に係る受信機の構成を示すブロック図である。

【図１０】本発明の第７の実施形態に係る受信機の構成を示すブロック図である。

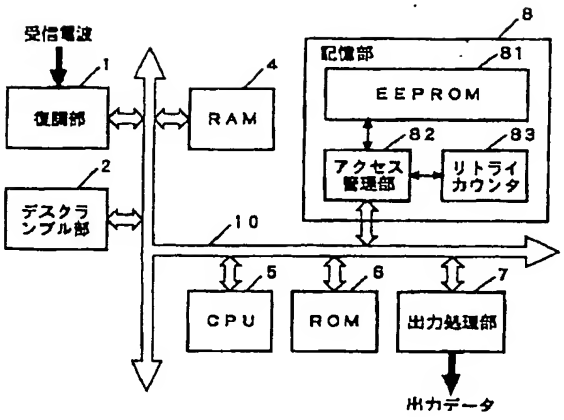
【図１１】他の状態遷移の一例を示す図である。

【図１２】従来の受信機の構成の一例を示すブロック図である。

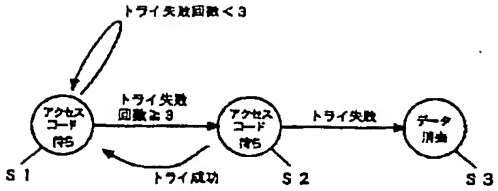
【符号の説明】

１、１０１…復調部
２、２ａ、１０２…デスクランブル部
３…ＩＤ付加部
４、１０４…ＲＡＭ
５、１０５…ＣＰＵ
６、１０６…ＲＯＭ
７、１０７…出力処理部
８、８ａ…記憶部
１０、１１０…バス
２６、２７…信号線
６１…ダウンロードモジュール（ＤＭ）
８１、１８１…ＥＥＰＲＯＭ
８２…アクセス監視部
８３…リトライカウンタ
８４…偽データＥＥＰＲＯＭ

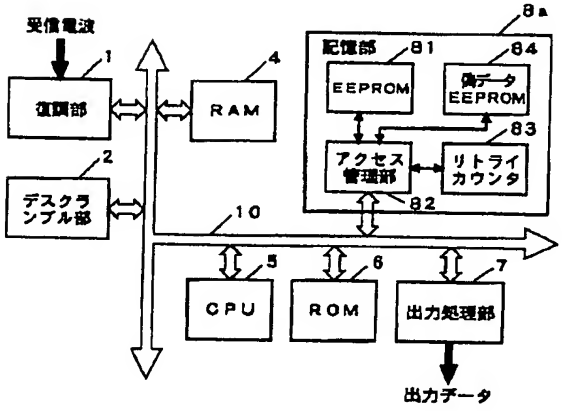
【図１】



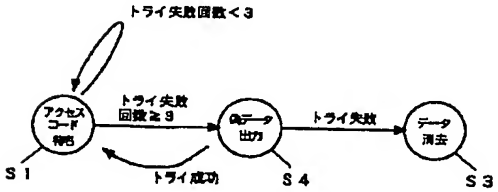
【図２】



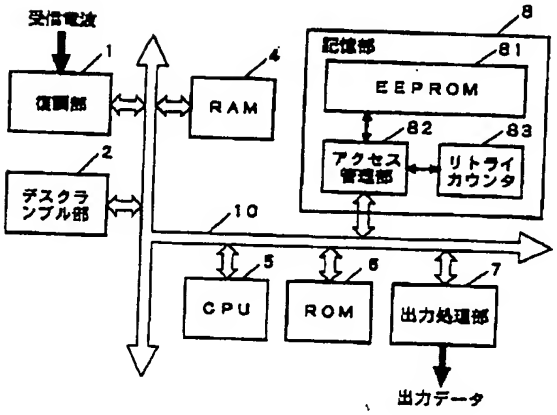
【図３】



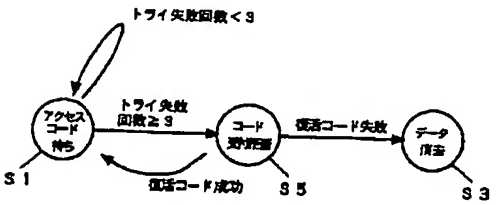
【図４】



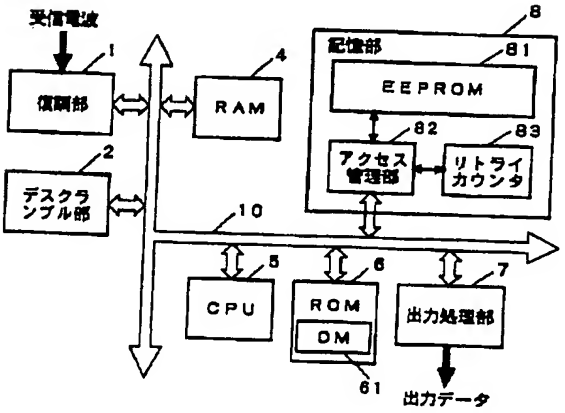
【図５】



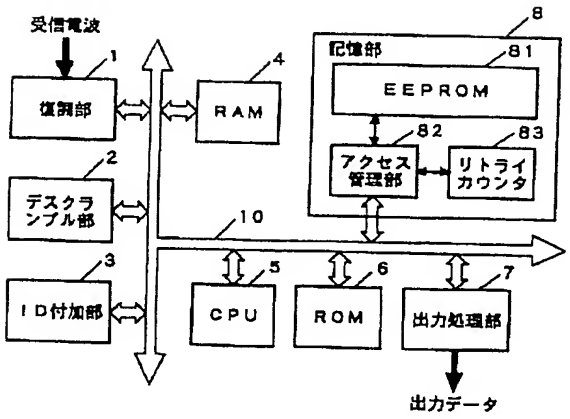
【図６】



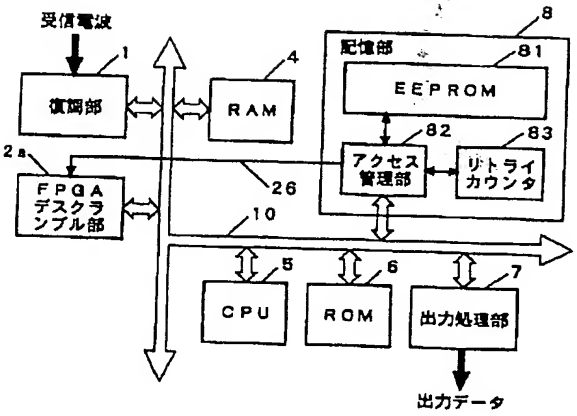
【図７】



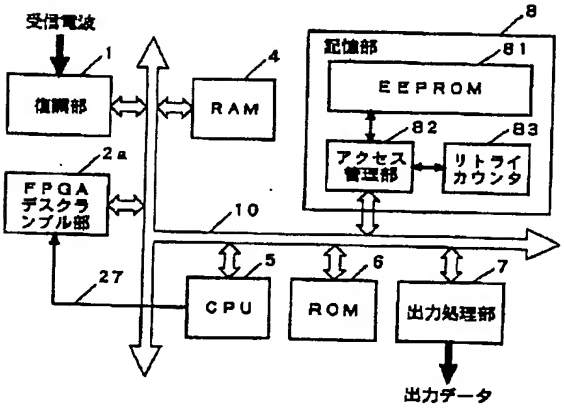
【図８】



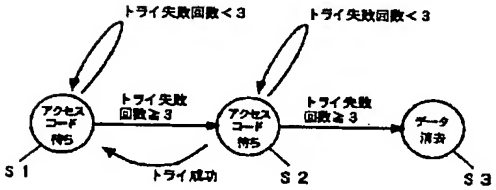
【図９】



【図１０】



【図１１】



【図１２】